UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/710,380 | 11/10/2000 | Arthur R. Hair | HAIR-22 | 5438 |

7590 04/29/2008

Ansel M Schwartz
One Sterling Plaza
201 N Craig Street
Suite 304
Pittsburgh, PA 15213

| EXAMINER | |
|---|---|
| DADA, BEEMNET W | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2135 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 04/29/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/710,380 | HAIR ET AL. | |
| | Examiner | Art Unit | |
| | BEEMNET W. DADA | 2135 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *01 February 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *17* is/are allowed.

6)☒ Claim(s) *1-4 and 9-16* is/are rejected.

7)☒ Claim(s) *5-8* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/29/08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on February 01, 2008 has been entered. Claims 1, 2, 13-16 have been amended and new claim 17 has been added. Claims 1-17 are pending.

### *Response to Arguments*

Applicant's arguments with respect to claims 1-16 have been considered but are moot in view of the new ground(s) of rejection.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4 and 9-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Olson et al. (U.S. Patent No. 6,311,209 B1) (hereinafter Olson) in view of Ballardie, "Scalable Multicast Key Distribution" April 1995 and further in view of Bruce Schneier, "Applied Cryptography" 2nd edition, 1996, pages 584-587.

As per claims 1 and 9-12, Olson teaches a system to establish a trusted and decentralized peer-to-peer network comprising:

communication means [figure 1, unit 12];

n user computing devices connected to the communication means, where n is greater than or equal to 3 and is an integer [figure 1 units 14, 16 and 18]; and

a host computing device connected to the communication means having a mechanism to establish a decentralized trusted communication network with at least 2 of the n users computing devices through which digital signals are shared (i.e. each client maintaining a copy of data throughout an application session, and each time client changes application data the change is communicated to all other clients, e.g. client A, B and C of Fig 1 maintaining a copy of data at elements 20, 22 and 24) [column 6, lines 29-41] securely between the host computing device and the 2 users computing devices of the trusted communication network [column 3, lines 30-41, column 6, lines 47-53 and column 2, lines 22-27], and further, the host computing device identifiable to the n user computing devices, the n computing devices and the host computing device forming a trusted member list that each computing device has and each computing device knows and can communicate directly with all the other computing device on the trusted peer-to-peer network (i.e., an application that includes a table containing unique identifiers for each clients participating in the session, see for example, column 3, lines 9-29).

Olson does not explicitly teach sending a public key to a first of the 2 user computer devices and the first user computing device sending a public key to a second of the 2 user computer devices through the communication means to establish the decentralized trusted network and the second user accepting or denying the public key in regards to joining the decentralized network. However, Ballardie teaches establishing a trusted decentralized peer-to-peer network including sending a public key from a host computing device to a first computing device through a communications means (i.e., page 8, C→B, sending group access package), sending the public key from the first user computing device to a second user computing device

connected to the communication means and receiving the key at the second user computing device (i.e., page 9, B→ A, A→ h, sending group access package) and the second computer accepting or denying the public key in regards to joining the decentralized trusted network [page 9]. One of ordinary skill in the art would have been able to modify the teachings of Ballardie within the system of Olson in order to distribute encryption keys in peer-to-peer environment. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the key distribution method taught by Ballardie within the secure decentralized system of Olson to achieve the advantage of providing key distribution in peer-to-peer environment between peer computing devices.

The combination of Olson and Ballardie is silent on the first user computing device sending public key to a second of the 3 user computer devices and a third of the 3 user devices through a communication means. However, Schneier teaches a decentralized based key distribution protocol, including a first user/device sending a public key to a second user/device and a third user/device and further including forming a trusted list that each user/device that each device has and each device knows and can communicate directly with all other devices in the list [see PGP trust model, pages 585-586]. Both Schneier and Olson-Ballardie are directed to a secure key distribution method in decentralized networks. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Schneier within the system of Olson-Ballardie in order to efficiently provide public keys in decentralized networks.

As per claims 2 and 13-16, Olson teaches a method of establishing a trusted and decentralized peer-to-peer network comprising the steps of:

sending a public key from a host computing device to communication means connected to the host computing device [column 3, lines 35-40];

establishing a decentralized trust communication network between the host computing device, a new client and existing clients by forwarding the public key to the new and existing clients [column 3, lines 35–40 and column 8, lines 12-21] through which digital signals are shared (i.e. each client maintaining a copy of data throughout an application session, and each time client changes application data the change is communicated to all other clients e.g. client A, B and C of Fig 1 maintaining a copy of data at elements 20, 22 and 24) [column 6, lines 29-41] securely between the host computing device and the client computing devices, and sending digital signals directly from the user computing device securely to the second computing device [column 3, lines 30-42, column 6, lines 47-53 and column 2, lines 22-27], and further, the host computing device identifiable to the n user computing devices, the n computing devices and the host computing device forming a trusted member list that each computing device has and each computing device know can communicate directly with all the other computing device on the trusted peer-to-peer network (i.e., an application that includes a table containing unique identifiers for each clients participating in the session, see for example, column 3, lines 9-29).

Olson does not explicitly teach sending a public key to a first of the 2 user computer devices and the first user computing device sending a public key to a second of the 2 user computer devices through the communication means to establish the decentralized trusted network and the second user accepting or denying the public key in regards to joining the decentralized network. However, Ballardie teaches establishing a trusted decentralized peer-to-peer network including sending a public key from a host computing device to a first computing device through a communications means (i.e., page 8, C→B, sending group access package), sending the public key from the first user computing device to a second user computing device

connected to the communication means and receiving the key at the second user computing device (i.e., page 9, B→ A, A→ h, sending group access package) and the second computer accepting or denying the public key in regards to joining the decentralized trusted network [page 9]. One of ordinary skill in the art would have been able to modify the teachings of Ballardie within the system of Olson in order to distribute encryption keys in peer-to-peer environment. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the key distribution method taught by Ballardie within the secure decentralized system of Olson to achieve the advantage of providing key distribution in peer-to-peer environment between peer computing devices.

The combination of Olson and Ballardie is silent on the first user computing device sending public key to a second of the 3 user computer devices and a third of the 3 user devices through a communication means. However, Schneier teaches a decentralized based key distribution protocol, including a first user/device sending a public key to a second user/device and a third user/device, receiving the public key at the third user device, and further including forming a trusted list that each user/device that each device has and each device knows and can communicate directly with all other devices in the list [see PGP trust model, pages 585-586]. Both Schneier and Olson-Ballardie are directed to a secure key distribution method in decentralized networks. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Schneier within the system of Olson-Ballardie in order to efficiently provide public keys in decentralized networks.

As per claims 3 and 4, the combination of Olson and Ballardie teaches the method as applied above. Furthermore, Ballardie teaches creating encryption and decryption keys [page 8-9].

## *Allowable Subject Matter*

Claim 17 is allowed.

Claims 5-8 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

## *Conclusion*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BEEMNET W. DADA whose telephone number is (571)272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Beemnet W Dada/
Art Unit 2135

April 22, 2008